

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED <div style="text-align: center; border: 1px solid black; padding: 2px;">TOP SECRET</div> b. LEVEL OF SAFEGUARDING REQUIRED <div style="text-align: center; border: 1px solid black; padding: 2px;">TOP SECRET</div>	
2. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i>				3. THIS SPECIFICATION IS: <i>(X and complete as applicable)</i>	
a. PRIME CONTRACT NUMBER		<input checked="" type="checkbox"/>		a. ORIGINAL <i>(Complete date in all cases)</i>	DATE (YYYYMMDD)
b. SUBCONTRACT NUMBER				b. REVISED <i>(Supersedes all previous specs)</i>	REVISION NO. DATE (YYYYMMDD)
c. SOLICITATION OR OTHER NUMBER		DUE DATE (YYYYMMDD)		c. FINAL <i>(Complete Item 5 in all cases)</i>	DATE (YYYYMMDD)
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract.					
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____.					
6. CONTRACTOR <i>(Include Commercial and Government Entity (CAGE) Code)</i>					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>	
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>	
NA		NA		NA	
8. ACTUAL PERFORMANCE					
a. LOCATION		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>	
SEE BLOCK 13					
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT					
Contractor Logistic Support for the _____ located at 58 TRSS, Kirtland, AFB, NM 19 SOS, Hurlburt Field, FL, and 193rd SOW, Middletown, PA.					
10. CONTRACTOR WILL REQUIRE ACCESS TO:		YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		<input checked="" type="checkbox"/>		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	
b. RESTRICTED DATA			<input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	
d. FORMERLY RESTRICTED DATA			<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	
e. INTELLIGENCE INFORMATION				e. PERFORM SERVICES ONLY	
(1) Sensitive Compartmented Information (SCI)		<input checked="" type="checkbox"/>		f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	
(2) Non-SCI		<input checked="" type="checkbox"/>		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	
f. SPECIAL ACCESS INFORMATION		<input checked="" type="checkbox"/>		h. REQUIRE A COMSEC ACCOUNT	
g. NATO INFORMATION		<input checked="" type="checkbox"/>		i. HAVE TEMPEST REQUIREMENTS	
h. FOREIGN GOVERNMENT INFORMATION		<input checked="" type="checkbox"/>		j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	
i. LIMITED DISSEMINATION INFORMATION			<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	
j. FOR OFFICIAL USE ONLY INFORMATION		<input checked="" type="checkbox"/>		l. OTHER <i>(Specify)</i>	
k. OTHER <i>(Specify)</i>				H-302 Clause "Notification of Government Security Activity" applies	

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (Specify)

PUBLIC RELEASE OF SCI IS NOT AUTHORIZED.

SAF/AQU Washington DC, 20330 and OO-ALC/PA, 7981 Georgia St, Hill AFB, UT 84056 (8 copies, 45 working days in advance of required date). Photocopies and audio materials are not acceptable.

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Contractor will be required to perform Contractor Logistics Support (CLS) in support of the operational and training requirements at multiple locations. Current locations are 58 TRSS Kirtland AFB, NM 87117, 19 SOS, Hurlburt Field, FL 32544, and 193rd SOW Middletown, PA 17057. Current Aircrew Training Devices (ATD) located at 58 TRSS include the following: MH-53J WST, H-53 PPT, MH-60G WST, HH/MH-60G OFT, MC-130P WST, MC-130H WST#1, MC-130H LMPTT, MC-130E LMPTT, UH-1N ROFT, AREIAL GUNNER SCANNER SIMULATOR (AGSS), CV-22 WST, CV-22 OFT, VISUAL THREAT RECOGNITION AVOIDANCE TRAINER (VTRAT) and all systems required to support the ATD's to include but not limited to the Audio Visual Studio, Data Base Facility, Courseware Development, Library and Training Observation Center (TOC). Current ATD's located at the 19 SOS are as follows: MC-130H WST#2, MC-130E WST, AC-130U WST, VTRAT, MH-53M WST, CV-22 OFT and all systems required to support the ATD's to include but not limited to Data Base Facility, Courseware Development, Library, and Mission Rehearsal Observation Center (MROC). Current ATD's located at 193rd SOW are as follows: EC-130E/J ATD, VTRAT, and all systems required to support the ATD's to include but not limited to the Data Base Facility, Courseware Development, and Library.

Classified taskings will be performed at the three locations and possibly at additional locations in the future. Unclassified taskings may be performed at the Contractors Facility located at:

(SEE ATTACHED CONTINUATION SHEET)

13a. Program Official

13b. Duty phone

Biennial Review Date

Timothy O'Brien

DSN 586-2846
(801) 586-2846

20070620

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. ☒ Yes ☐ No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

Provide the information requested by the Notification of Government Security Activity Clause, AFFARS 5352.204-9000, to the Servicing Security Activity (SSA) address in block 17 of this form. Refer to contract document for these clauses. SEE ATTACHED

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. ☒ Yes ☐ No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

SEE ATTACHED

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL

b. TITLE

c. TELEPHONE (Include Area Code)

Ramon Castillo

Contracting Officer

(801) 586-0682

d. ADDRESS (Include Zip Code)

508 MASSG/PK
6072 Fir Ave
Hill AFB, UT 84056-5825

e. SIGNATURE

17. REQUIRED DISTRIBUTION

- | | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | a. CONTRACTOR |
| <input type="checkbox"/> | b. SUBCONTRACTOR |
| <input checked="" type="checkbox"/> | c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR |
| <input type="checkbox"/> | d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION |
| <input type="checkbox"/> | e. ADMINISTRATIVE CONTRACTING OFFICER |
| <input checked="" type="checkbox"/> | f. OTHERS AS NECESSARY |

DD FORM 254 continued

Ref. 8.a. Actual Performance Location:

58TRSS	19 th SOS	193 rd SOW
1960 Eileen Ave	589 Independence Rd	81 Constellation Court
Kirtland AFB, NM 87117-5301	Hurlburt Fld, FL 32544-9340	Middletown, PA 17057

Note: There may be additional sites in the future.

Ref. 10.a. COMSEC material/information may not be released to DOD contractors without Air Force Cryptological Support Center (AFCSC) approval. Contractor must forward request for COMSEC material/information to the COMSEC officer through the program office. The contractor is governed by the DOD 5220.22-S COMSEC Supplement to the NISPOM in the control and protection of COMSEC material/information. Access to COMSEC material by personnel is restricted to U.S. citizens holding final U.S. Government clearances. Such information is not releasable to personnel holding only reciprocal clearances.

Ref. 10.e. (1) Contractor will require access to DCID's 1/7 and 1/9.

Ref. 10.f. DSS maintains cognizance over the SAP. The inspecting Industrial Security Representative must be briefed into the ATARS SAP program by the government program manager or designated representative prior to access to the SAP material.

Ref. 10.g. Access to classified NATO information requires a final U.S. Government clearance at the appropriate level, and a NATO briefing.

Ref. 10.h. Access requires a final U.S. Government clearance at the appropriate level.

Ref. 10.j. FOUO information provided under this contract shall be safeguarded as specified in the attachment Protecting For Official Use Only (FOUO) Information.

Ref. 11.c. The contractor requires access to classified source data up to and including **TOP SECRET** in support of the work effort. Any extracts or use of such data requires the contractor to apply derivative classifications and markings consistent with the source documents. Use of Multiple Sources on the classified by line necessitates compliance with the NISPOM, and use of bibliography.

Ref. 11.g. The contractor must prepare and process a DD Form 1540 and 2345 for request to utilize the Defense Technical Information Center (DTIC). Reference the NISPOM for preparation and processing of these forms.

Ref. 11.h. A COMSEC account will be established and COMSEC will be protected per DoD 5220.22-S.

Ref. 11.i. See attached addendum.

Ref. 11.j. See Addendum A for additional OPSEC requirements.

Ref. 11.k. The contractor must request DCS services from:

Commander, Defense Courier Service
Attn: Operations Division
Fort George G. Meade, MD 20755-5370

Ref. 13.

1. Items 11e, 11f, 11g, and 11h apply to the Hurlburt Field site only.
2. Security Classification Guide.
See attached list of Security Classification Guides.
3. PERSONNEL: The contractor shall be responsible for obtaining and maintaining the proper clearances for contractor personnel. The contractor personnel assigned under this contract are required to have a current security clearance and compatible level of access IAW DD Form 254. Current security clearance requirements are SECRET and TOP SECRET at 19 SOS, Hurlburt Field FL. SECRET at 58 TRSS, Kirtland AFB NM, and SECRET at 193rd SOW, Middletown PA. The contractor personnel shall have the required security clearance prior to arrival on-site.
4. ASSIGNMENT OR CHANGE: Assignment or changes of contractor personnel to Kirtland AFB shall be the responsibility of the contractor. The following information shall be provided to Kirtland AFB when changes/assignments occur prior to arrival on site: name, social security number, date and place of birth, citizenship, position, date of assignment, type of security clearance, are issued and agency granting the clearance. This information shall be IAW Kirtland AFB requirements.
5. OPERATIONS SECURITY: The contractor shall conduct an Operations Security (OPSEC) analysis and implement an OPSEC Plan
6. CLASSIFIED/SENSITIVE SHIPMENTS: The contractor shall be responsible for the shipment of Classified/Sensitive material/data and shall assure such shipments are protected IAW DoD National Industrial Security Program Operating Manual (NISPOM) 5220.22M
7. COMPUTER SECURITY: Computer security for the ATARS effort shall be IAW AFD 33-2 C4 system security.
8. TRAINER FACILITY ACCESS: The contractor shall be responsible for the security of the ATARS equipment facilities normally manned by contractor personnel, and shall be responsible for access control to the facility and shall be responsible for securing the facilities upon leaving IAW established site base procedures. The contractor shall escort visitors through the facilities at the governments' request. The contractor shall provide the Project Officer a point of contact for access to the trainer areas during non-duty hours. All requests for non-duty access shall be coordinated through the PO or designated alternate. The contractor shall escort contract janitorial services personnel, if required, and authorized personnel performing maintenance/upkeep the trainer area. In case of an emergency during non-duty hours, the PO/QAR or building custodian may provide access to the trainer site for emergency personnel, if contractor personnel are not available. The contractor shall control and provide access up to 24 hours per day, including Saturdays and Sundays for government personnel on an on-call basis. Access for other contractors in performance of modifications, maintenance and inspections will be provided during times agreed to by the Air Force and ATARS contractor as defined in the Associate Contractor Agreement (ACA).
9. PHYSICAL SECURITY: The contractor shall be responsible for safeguarding all government property provided for contractor use. At the close of each work period, government facilities, equipment and materials shall be secured.
10. KEY CONTROL: The contractor shall establish and implement procedures to ensure that all keys/cards issued to the contractor by the Government are not lost, misplaced, duplicated or used by unauthorized persons. The contractor shall report the occurrences of a lost or duplicated key/card to the PO when known. In the event that keys/cards, other than master keys/cards, are lost or duplicated, the contractor shall be required, upon direction of the PO, to re-key/card or replace the affected lock(s). The Government, at its option, may replace the affected locks or perform re-keying. When the replacement of locks or rekeying is performed by the Government, the total cost of re-keying or card replacement or replacement of the locks will be deducted from the monthly payment due the contractor.

11. COMBINATION CONTROL: The contractor shall establish, implement and maintain methods of ensuring that all lock combinations are not revealed to unauthorized persons. The contractor shall develop procedures covering combination control IAW DoD 5220.22M.
12. VISITOR NOTIFICATION: All requests for visitor access to the training facility shall be coordinated through the PO.

Ref. 14. (Ref. 10.e.1)

Contract monitor is:

Special Security Officer (SSO) is:

Ramon Castillo
508 MASSG/PK
6072 Fir Ave
Hill AFB UT 84056-5825
(801) 777-8114

Ms. Vickie Wehus
OO-ALC/XPI
6137 Wardleigh Way
Hill AFB UT 84056-5843
(801) 777-0484

Ref. 14. See attached SCI Release of Intelligence Information for additional security requirements. Prior approval of the contracting activity is required for subcontracting. Access to intelligence information requires special briefing and an U.S. Government clearance at the appropriate level.

Ref 15. (Ref. 10.e.) The 19 SOS/DOF Hurlburt Field FL has exclusive security responsibility for all SCI classified material released to or developed under this contract and held within the contractor's SCIF. DSS is relived of security inspection responsibility for all such material but retains responsibility for all non-SCI classified material released to or developed under the contract and held within the documentation to ensure compliance with SCI directives or regulations.

Ref 15.

- a) The 377 SFS/SFA is the cognizant security office for work performed at Kirtland AFB NM and will perform industrial security inspections required during performance of this contract.
- b) The 16 SFS Hurlburt Field, FL is the cognizant security office for work performed at Hurlburt Field FL and will perform industrial security inspections required during performance of this contract.
- c) The 193 SFS is the cognizant security office for work performed at Middletown PA and will perform industrial security inspections required during performance of this contract.

Ref. 17f. OTHERS AS NECESSARY (DD Form 254 only)

75 SFS/SFAI
Elizabeth West

508 ASW/OMO
Annette Burrell

75 CS/SCBNS
Lori Prendergast

84 MSUG/GBMSH
David Page

SFS/SFAI
Karl Abbott

OO-ALC/XPI
Vickie Wehus

**List of Applicable
Security Classification Guides**

GUIDE	DATE	OPR	POINT OF CONTACT
MH-53M WEAPONS SYSTEM TRAINER (WST)	4-NOV-03	ODGEN ALC	YWS/Mark Moulding 777-7103
MH-53J HELICOPTER	1-Sep-99	WARNER ROBINS ALC	
MH-53J WEAPON SYSTEM TRAINER (WST)	20-Jun-03	ODGEN ALC	YWS/Tim O'Brien 586-2846
HH/MH-60G PAVE HAWK HELICOPTER	1-Aug-96	WARNER ROBINS ALC	LU/Rick Coogle 468-7261
MH-60G WEAPON SYSTEM TRAINER (WST)	1-Mar-05	ODGEN ALC	YWS/Tim O'Brien 586-2846
MC-130P/N TANKER AIRCRAFT	22-May-88	WARNER ROBINS ALC	
MC-130P WEAPON SYSTEM TRAINER (WST)	1-Mar-05	ODGEN ALC	YWS/Tim O'Brien 586-2846
COMBAT TALON	28-Dec-88	WARNER ROBINS ALC	LU/Mike Edwards 468-2566
CV-22	10-Jul-00	COMNAVAIRSYSCOM	
HAVE QUICK/II/IIA	1-Jun-90	HANSCOM AFB MA	ESC/TGH Erwin Day 478-8931
AN/ALQ-162		NAVAIR	TONI NAPPER
AN/ALQ-157		NAVAIR	TONI NAPPER
AN/ALR-69(V) Radar Warning Receiver (RWR)	14-Feb-97	WARNER ROBINS ALC	LN/WAYNE HALL
AN/ARC-190 HF Communications System	25-Aug-97	WARNER ROBINS ALC	Jim Clance 468-9431
AN/AAQ-18 INFRARED DETECTING SET	1-Mar-91	WARNER ROBINS ALC	Luther McKinley 468-9374
AN/AAR-47	14-Mar-96	WARNER ROBINS ALC	LN/Ben Blanchard 468-7228
KY 75 Secure Voice & KY-58/75 SATCOM system			
AN/ARC-164 (V) SATCOM radio			
AN/APR-39A(V)-1 RWR	5-Oct-99	Aircraft Survivability Equipment (ASE),	
AN/ALQ-144(V)-2 ICRM	14-May-02	Aircraft Survivability Equipment (ASE),	
ASN-149 GPS		HQ Space and Missile Systems	
AAQ-16 FLIR			
IDAS/MATT	25-Oct-96	Warner Robins ALC	
SCG SOFATS	10-Jan-90		
AN/AAR-44 Infrared Warning Receiver	14-Jul-00	WR/ALC	MMR/Jacquelyn Simpson 468-5804
AN/ALR-46(V) Radar Warning Receiver	1-Aug-99	WR/ALC	LNR/Wayne Hall 468-6136
AN/ALR-46(V) Infrared Warning Receiver	3-May-88	WR/ALC	LNR/Wayne Hall 468-6136
AN/ALQ-172(V) Electronic Countermeasure	21-Aug-00	WR/ALC	MMRMB/Bob Boyle 468-4960
AN/ALR-74 Radar Warning Response	1-Jun-86	Wright Patterson AFB	ASD-YPD 785-4385
AN/ALR-196 Program	1-Jun-88	Wright Patterson AFB	AFLC-AZ (513)257-6251
AN/APM-427 Improved Radar Simulator	1-Mar-97	WR/ALC	MMR/Paul Cosey 468-6136
AN/USM-464 Counter Measures Test Set	1-Jul-97	WR/ALC	MMRBM/Marvin Brown 468-4960
QRC 84-02A ICRM Set	1-Apr-97	WR/ALC	MMRMP/J. Schechterle 468-5804
QRC-84-02A Radar Warning Receiver	1-Oct-89	WR/ALC	MMRMP/J. Schechterle 468-5804
MH-53J Helo SCG	1-Sep-99	WR/ALC	Edward Cigahn/468-7945

AC-130H Gunship Aircraft	1-May-03	WR/ALC	LUG/468-6310
AC-130U Gunship Replacement	30-Jun-03	Wright Patterson	ASC-LU/785-4152
Combat Talon I and II	28-Dec-87	WR/ALC	LUM/468-2698
AN/ALR-69V Radar Warning Receiver	1-Aug-99	WR-ALC/LNR	Wayne Hall
AN/ARC-190 HF Communication Systems	25-Aug-97	WR/ALC	LYLCL 468-9431
Visual Threat and Recognition Avoidance Trainer (VTRAT)	21-Mar-03	AFSOC	SMSgt Philip Bean 579-2240
MC-130H WST	31-Jul-85	OO/ALC	YWS/Tim O'Brien 586-2846
53J Integrated Electronic Warfare System	1-May-98	WR/ALC	
AN/AAQ-17 Infrared Detecting Device	30-Sep-97	WR/ALC	
AN/APM-427 Improved Radar Simulation	1-Mar-97	WR/ALC	MMR/Paul Cosey 468-6136
AGSS SCG	1-Mar-94		
EC-130E/J Commando Solo	1-Apr-01	HQ AFSOC	DOXP

SENSITIVE COMPARTMENTED INFORMATION (SCI)
Reference DD Form 254 Item 10e(1)

- 1 This contract required additional security requirements for Sensitive Compartmented Information (SCI) IAW DoD 5105.21-M-1 and AFMAN 14-304. The Assistant Chief for Intelligence, Headquarters United States Air Force (USAF/IN) has exclusive security responsibility for all SCI classified material released to or developed under this contract.
- 2 The following documents, with subsequent versions or changes, will be used for the specific guidance on this contract:
 - a) DoD Directive 5105.21-M-1, SCI Administrative Security Manual.
 - b) AFMAN 14-304, The Security, Use, and Dissemination of SCI.
 - c) DCID 6/6, Security Controls on the Dissemination of Intelligence Information.
 - d) DCID 6/1, Security Policy for Sensitive Compartmented Information (SCI).
 - e) DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities.
 - f) DIAM 50-4, DoD Intelligence Information System (DoDIIS) Information Systems Security Program.
 - g) DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems.
 - h) Joint DoDIIS/Cryptologic SCI Information Systems Security Standards
 - i) AFI 14-304, Release of Collateral Intelligence to US Contractors and Supplements.
- 3 Inquires pertaining to classified guidance on Sensitive Compartmented Information (SCI) will be directed to the responsible Supporting SSO indicated. Any SCI or SCI derived material generated under this contract will be reviewed by the Supporting SSO for proper SCI classification prior to final publication and distribution. The responsible Special Security Office designated will provide assistance as required.
- 4 SCI data furnished to or generated by the contractor will require special security handling and controls beyond those of the NISPOM. These supplemental instructions will be furnished and/or made available to the contractor through the Contract Monitor by the User Agency SSO.
- 5 The names of contractor personnel requiring access to SCI will be submitted to the Contract Monitor for approval. Upon written approval by the Contract Monitor, forms requesting Special Background Investigations will be prepared in Accordance with NISPOM and then submitted to the Supporting SSO (OO-ALC/XPI).
- 6 The contractor will establish and maintain an access list of those employees working on the contract. A copy of this will be furnished to the Contract Monitor.
- 7 The contractor will advise the Contract Monitor immediately upon reassignment of personnel to other duties not associated with this contract.
- 8 SCI will not be released to the contractor employees without the specific consent of the Supporting Senior Intelligence Officer or the originator of the material when applicable. This approval will be obtained through the Supporting SSO (OO-ALC/XPI) based on prior approval and certification of need-to-know by the Contract Monitor. SCI documentation, or other material concerning this contract will not be discussed with, released to, any individual, subcontractor, agency (including Federal Government agencies and employees), or contractor employees not working on the contract without prior written approval from the Contract Monitor and Supporting SSO.

- 9 Any SCI released to or generated by the contractor in support of this contract remains the property of the DoD department, agency, or command that released it. The contractor will release such material to any Special Security Office personnel assigned to OO-ALC/XPI, HQ AFMC/IN, HQ USAF/IN, or DIA upon demand by such personnel. The contractor will maintain a record of all SCI material released to his custody under this contract and upon completion/cancellation of the contract, must return all such material to the Supporting SSO. This applies to all data and materials, including working papers and notes.
- 10 Contract Monitors and Contract Special Security Officers (CSSOs) will comply with all requirements in the Contract Monitors Handbook.
- 11 The contractor will not reproduce any SCI related to this contract without written permission from the Contract Monitor and Supporting SSO except for working papers and derivative material produced in the publication process. Working papers and derivative material produced in the publication process do not need destruction approval. When such permission has been granted, the contractor will control and account for such reproductions IAW DoD-5105-21-M-1 and AFMAN 14-304.
- 12 (ONLY USE IF A CONTRACTOR SCIF IS REQUIRED). A Sensitive Compartmented Information Facility (SCIF) will be established IAW DCID 6/9 at the contractors facility and will be maintained by the contractor. SCI material associated with this contract will be stored in approved safes and maintained only in a properly DIA accredited SCIF at the contractor or government facility. The contractor will maintain a full time CSSO at the contractor's SCIF who will be directly responsible to the Program Manager and the Supporting SSO for security.
- 13 (ONLY USE IF ELECTRONIC PROCESSING OF SCI IS REQUIRED). The contract requires electronic processing of SCI. In addition to the security provisions outlined in DCID 6/4, additional security provisions of DCID 6/9, AFMAN 14-304, and the Joint DoDIIS/Cryptologic SCI Information Systems Security Standards apply, and are part of this contract. The contractor's Automatic Data Processing Equipment (ADPE) must be accredited for SCI operations from DIA via the Supporting SSO prior to processing any SCI material.
- 14 The contractor will not use reference to SCI access, even by unclassified acronyms, in advertising, promotional efforts, or recruitment for employees.
- 15 Contractor must coordinate with the Supporting SSO and obtain the concurrence of the Contract Monitor prior to subcontracting any portion of the SCI efforts involved in this contract.
- 16 The contractor will comply with AFFAR 5352.204.9001 clause for AFB visits.

Non-Sensitive Compartmented Information (SCI)
Reference DD Form 254 Item 10e (2)

- 1 Special Requirements Of Intelligence Information: The contractor will require access to, and receipt of, classified intelligence documents in the performance of this contract. In addition to the requirements and controls for classified material in DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), the contractor shall adhere to the following requirements and controls of intelligence, per AFI 14-303 and applicable supplements.
- 2 Contact OO-ALC/XPI, 6137 Wardleigh Rd., Hill AFB UT 84056-5843, the Unit IN for permission to make extra copies of intelligence data required by the contractor if approval has not previously been stipulated above or been stipulated in the release letter. The Contract Monitor (CM) then maintains accountability of copies and ensures all information is returned to the Air Force upon contract termination/expiration.
- 3 Maintain a record of all intelligence materials released to the contractor, and ensures all data is returned to the CM within 2 years after final delivery of goods and services or after completion or termination of the classified contract, whichever comes first. If retention is required beyond the 2 year period the contractor must request and receive written authority from the CM.
- 4 Contractor shall maintain accountability for all intelligence released in his/her custody. Contractors must agree that all intelligence data released to them, all reproductions, and other material generated (including authorized reproductions) is the property of the US Government and will be returned upon request of the sponsoring agency or expiration date of the contract, whichever comes first.
- 5 Contractor shall not reproduce intelligence without permission from the Unit IN (OO-ALC/XPI) through the CM. If approved, must control each copy in the same manner as the original.
- 6 Contractor shall not reproduce intelligence without advance approval from the CM, except for working papers and derivative material produced in the publication process. Working papers and derivative material produced in the publication process do not need destruction approval.
- 7 Contractor shall restrict access to those individuals with a valid need-to-know who are actually providing services under the contract. Further dissemination to other contractors, subcontractors, or other government agencies and private individuals or organizations is prohibited unless authorized in writing by the CM with prior approval of the Unit IN (OO-ALC/XPI)/contracting activity.
- 8 Contractor shall not release intelligence data to foreign nationals or immigrant aliens regardless of their security clearance or contract status without advanced written permission from the CM, Unit IN (OO-ALC/XPI), Foreign Disclosure Policy Office, and HQ AFMC/IN.

- 9 Contractor shall ensure the each employee having access to intelligence material is fully aware of the special security requirements for this material and maintains records in a manner that permits the contractor to furnish on demand the names of individuals who have access to the material in their custody.
- 10 Releasing authority of intelligence documents is HQ AFMC/IN. Any request for intelligence documents will be sent through the CM to the Unit IN (OO-ALC/XPI) designee for HQ AFMC/IN for approval.

FOR OFFICIAL USE ONLY (FOUO)

REF. to Item 10j

FOUO is not a classification. Originators mark records when they create them to call attention to FOUO content. An FOUO marking does not mean you must withhold a record under the FOIA. You still need to review a requested record. Examine records with and without markings to identify information that needs protection and is exempt from public release or to decide whether discretionary release is appropriate.

Information in a technical document that requires a distribution statement per AFI 61-204, Disseminating Scientific and Technical Information, must show that statement. The originator may also mark the information FOUO, if appropriate.

Mark an unclassified document containing FOUO information "For Official Use Only" at the bottom, on the outside of the front cover (if any), on each page containing FOUO information, on the back page, and on the outside of the back cover (if any).

In unclassified documents, the originator may also mark individual paragraphs that FOUO information to users and assist in review.

In a classified document, mark:

- An individual paragraph that contains FOUO, but not classified information, by placing "(FOUO)" at the beginning of the paragraph.
- The top and bottom of each page that has both FOUO and classified information, with the highest security classification of information on that page.
- "FOUO" at the bottom of each page that has FOUO but not classified information.

If a classified document also contains FOUO information or if the classified material becomes FOUO when declassified, place the following statement on the bottom of the cover or the first page, under the classification marking: "NOTE: If declassified, review the document to make sure material is not FOUO and not exempt under AFI 37-131 before public release."

Mark other records, such as computer printouts, photographs, films, tapes or slides, "For Official Use Only" or "FOUO" so the receiver or viewer knows the record contains FOUO information.

Mark FOUO material sent to authorized persons outside the DoD with an explanation typed or stamped on the document.

DoD components, officials of DoD components, and authorized DoD contractors, consultants, and grantees send FOUO information to each other to conduct official DoD business. Tell recipients the status of such information, and send material in a way that prevents unauthorized public disclosure. Make sure documents that transmit FOUO material call attention to any FOUO attachments. Normally, you may send FOUO records over facsimile equipment. To prevent unauthorized disclosure, consider attaching special cover sheets (i.e. AF Form 3227, Privacy Act Cover Sheet, for Privacy Act Information), the location of sending and receiving machines, and whether authorized personnel are around to receive FOUO information. FOUO information may be passed to officials in other departments and agencies of the executive and judicial branches to fulfill a government function. Mark the records "For Official Use Only", and tell the recipient the information is exempt from public disclosure under the FOIA and whether it needs special handling.

When you use the US Postal Service, package records with FOUO information so their contents are safe. If FOUO information is not combined with classified information, individuals may send FOUO information by First Class Mail or Parcel Post. Bulky shipments, such as FOUO directives to testing materials, that qualify under postal regulations may be sent by Fourth Class Mail.

Mark each part of a message that contains FOUO information. Unclassified messages containing FOUO information must show the abbreviation "FOUO" before the text begins.

To safeguard FOUO records during normal duty hours, place them in an out-of-sight location if people who do not work for the government come into the work area. After normal duty hours, store FOUO records to prevent unauthorized access. File them with other unclassified records in unlocked files or decks, etc., if the Government or a Government contractor provides normal internal building security. When there is no internal security, locked buildings or rooms usually provide adequate after-hours protection. For additional protection, store FOUO material in locked containers such as file cabinets, desks, or bookcases.

When a record is no longer FOUO, remove the markings or indicate on the document the markings no longer apply. Try to tell everyone who has the records that their status has changed.

Destroy FOUO materials by tearing them up so no one could put them back together and throwing them into trash containers. When the information needs more protection, local authorities may use other methods. However, balance the expense of extra protection against the degree of sensitivity of the FOUO information in the records. You may recycle FOUO material. Safeguard the FOUO documents or information until recycling to prevent unauthorized disclosure

Unauthorized disclosure of FOUO records is not an unauthorized disclosure of classified information. Personnel must act to protect FOUO records under their control from unauthorized disclosure. When unauthorized persons gain access to these records, administrators find out who is responsible and take disciplinary action where appropriate. Unauthorized disclosure of FOUO information containing PA information may also result in civil or criminal sanctions against individuals. Tell the originating organization when its records are improperly disclosed.

EMSEC Requirements
Addendum to DD Form 254, Item 11I
EMISSIONS SECURITY ASSESSEMENT REQUEST (ESAR)
FOR ALL CLASSIFIED SYSTEMS

a The contractor shall ensure that compromising emanations (EMSEC) conditions related to this contract are minimized

b The contractor shall provide countermeasures assessment data to the Contracting Officer (CO), in the form of an EMSEC Countermeasures Assessment Request (ESAR), the ESAR shall provide only specific responses to the data required in paragraph c, below. The contractors standard security plan shall **NOT** be used as a stand-alone ESAR response. The contractor shall **NOT** submit a detailed facility analysis/assessment. The ESAR information will be used to complete an EMSEC Countermeasures Assessment Review of the contractors facility to be performed by the government EMSEC authority using current Air Force EMSEC directives. EMSEC applies on a case-by-case basis and further information may be required to complete the review; should this be the case the contractor shall provide this information to the contracting officer when requested. After the evaluation of the ESAR by the government EMSEC authority, additional EMSEC requirements may be necessary. When changes to the information required in paragraph c, below occur (including, but not limited to, relocation of equipment from the original approved room) the contractor shall notify the contracting officer of these changes. The contractor shall submit to the CO a new ESAR, identifying the new configuration at least thirty (30) days before the changes occur, the contractor shall not commence processing with the new configuration until receiving approval from the contracting officer.

c *ESAR contents shall include, as a minimum, the following information (NISPOM, para 11-101c):

- 1) The specific classification and special categories of material to be processed/handled by electronic means.
- 2) The percentage of information being processed. Identify the approximate percentage for each level of information processed including unclassified.
- 3) The specific location where classified processing will be performed. (Include identification of any other contractor/company/agency located within 200 meters of the facility [building, room or office where classified processing is taking place]. Also, attach a copy of DIS Form 147. Record in block 15 the type and location relative to the system of any unfiltered telephone or communications lines, underground or unfiltered power lines, conduit, heating and air conditioning, water pipes, etc., that transgress the established area).
- 4) The name, address, title, and telephone number of point-of-contact the facility where processing will occur.

d The prime contractor shall ensure that all sub-contractors and/or vendors comply with EMSEC requirements when performing classified processing related to this contract. They will provide the above documentation through their prime to the contracting officer to complete the ESAR.

*NOTE: A copy of your Automated Information System Security Plan(s) (AISSP) will suffice.

OPERATIONS SECURITY (OPSEC) PARTICIPATION FOR CONTRACTORS

General:

OPSEC is a systematic means of identifying and protecting bits and pieces of information which an adversary could use to their advantage or our disadvantage.

Critical information is the information which has been identified by the OPSEC program as requiring protection.

OPSEC measures (formerly countermeasures) are control standards with which all personnel must comply in order to protect critical information. For example, personnel may be prohibited from discussing certain subjects via unencrypted telephones.

Responsibilities:

The contractor will give initial and recurring (annual) briefing/training to all personnel assigned to their organizations. All personnel must participate in the appropriate OPSEC programs. Participation includes ensuring all personnel attend and comply with the OPSEC training provided by the Responsible Agency, Organization, Program, or Facility for the contract. This training must provide listings of critical information that must be protected by all personnel, listings of OPSEC measures which must be used by all personnel to protect critical information, foreign intelligence and industrial espionage threats, OPSEC fundamentals and principles, and the importance of OPSEC to the overall information operations mission. All personnel must comply with OPSEC standards and practices as trained. All personnel must report OPSEC related incidents, issues and concerns to the OPSEC manager as identified in training. Training must be provided before personnel are allowed access to critical information. Training must be conducted annually thereafter, or as individual programs require. Additional training may be required based on updates to critical information, OPSEC measures, intelligence threat, access requirements, or other fundamental changes to the OPSEC program.

